

GUTRIDE SAFIER LLP

Seth A. Safier (State Bar No. 197427)

seth@gutridesafier.com

Marie A. McCrary (State Bar No. 262670)

marie@gutridesafier.com

Todd Kennedy (State Bar No. 250267)

todd@gutridesafier.com

Kali R. Backer (State Bar No. 342492)

kali@gutridesafier.com

100 Pine Street, Suite 1250

San Francisco, CA 94111

Telephone: (415) 639-9090

Facsimile: (415) 449-6469

Attorneys for Plaintiff

UNITED STATES DISTRICT COURT

NORTHERN DISTRICT OF CALIFORNIA

JONATHAN GABRIELLI, an individual, on
behalf of himself, the general public, and those
similarly situated,

Plaintiff,

v.

HALEON US INC.,

Defendant.

CASE NO.

**CLASS ACTION COMPLAINT FOR
INVASION OF PRIVACY; INTRUSION
UPON SECLUSION; WIRETAPPING IN
VIOLATION OF THE CALIFORNIA
INVASION OF PRIVACY ACT
(CALIFORNIA PENAL CODE § 631);
USE OF A PEN REGISTER IN
VIOLATION OF THE CALIFORNIA
INVASION OF PRIVACY ACT
(CALIFORNIA PENAL CODE § 638.51);
COMMON LAW FRAUD, DECEIT
AND/OR MISREPRESENTATION;
UNJUST ENRICHMENT; AND
TRESPASS TO CHATTELS**

JURY TRIAL DEMANDED

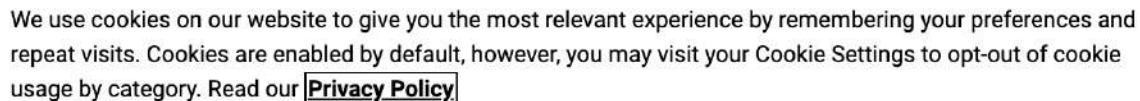
TABLE OF CONTENTS

INTRODUCTION	3
THE PARTIES.....	4
JURISDICTION AND VENUE	5
SUBSTANTIVE ALLEGATIONS	5
A. Defendant Programmed the Websites to Include Third-Party Resources that Utilize Cookie Trackers.	5
B. Defendant Falsely Informed Users That They Could Reject the Websites’ Use of Cookies.	10
C. The Private Communications Collected As a Result of Third Party Cookies Transmitted When Visiting Defendant’s Websites.....	14
1. Google YouTube Cookies.....	14
2. Microsoft Clarity Cookies.....	19
3. RevTrax Cookies	22
D. The Private Communications Collected are Valuable.	22
PLAINTIFF’S EXPERIENCES	24
TOLLING	26
CLASS ALLEGATIONS	27
CAUSES OF ACTION.....	29
First Cause of Action: Invasion of Privacy.....	29
Second Cause of Action: Intrusion Upon Seclusion.....	31
Third Cause of Action: Wiretapping in Violation of the California Invasion of Privacy Act (California Penal Code § 631).....	33
Fourth Cause of Action: Use of a Pen Register in Violation of the California Invasion of Privacy Act (California Penal Code § 638.51)	38
Fifth Cause of Action: Common Law Fraud, Deceit and/or Misrepresentation.....	39
Sixth Cause of Action: Unjust Enrichment.....	42
Seventh Cause of Action: Trespass to Chattels	43

Plaintiff Jonathan Gabrielli (“Plaintiff”) brings this action on behalf of himself, the general public, and all others similarly situated against Haleon US Inc. (“Defendant” or “Haleon”). Plaintiff’s allegations against Defendant are based upon information and belief and upon investigation of Plaintiff’s counsel, except for allegations specifically pertaining to Plaintiff, which are based upon Plaintiff’s personal knowledge.

INTRODUCTION

1. This Class Action Complaint concerns an egregious privacy violation and total breach of consumer trust in violation of California law. When consumers visit Defendant’s websites (including, tums.com; advil.com; centrum.com; theraflu.com; caltrate.com; flonase.com; sensodyne.com; and emergenc.com; each a “Website” and collectively, the “Websites”), Defendant displays to them a popup cookie consent banner. Defendant’s cookie banners disclose that the Websites use cookies but expressly gives users the option to control how they are tracked and how their personal data is used. Defendant assures visitors that they can choose to “Reject All” cookies as shown in the following screenshot:



We use cookies on our website to give you the most relevant experience by remembering your preferences and repeat visits. Cookies are enabled by default, however, you may visit your Cookie Settings to opt-out of cookie usage by category. Read our [Privacy Policy](#)

[Cookie Settings](#)

Reject All

Accept Cookies

2. Like most internet websites, Defendant designed the Websites to include resources and programming scripts from third parties that enable those parties to place cookies and other similar tracking technologies on visitors’ browsers and devices and/or transmit cookies along with user data. However, unlike other websites, Defendant’s Websites offer consumers a choice to browse without being tracked, followed, and targeted by third party data brokers and advertisers. However, Defendant’s promises are outright lies, designed to lull users into a false sense of security. Even after users elect to “Reject All” cookies, Defendant surreptitiously enables several third parties – including Google LLC (YouTube), Microsoft Corporation

(Clarity), and Neptune Retail Solutions (RevTrax) (the “Third Parties”) – to place and/or transmit cookies that track users’ website browsing activities and eavesdrop on users’ private communications on the Websites.

3. Contrary to their express rejection of cookies and tracking technologies on the Websites, Defendant nonetheless caused cookies, including the Third Parties’ cookies, to be sent to Plaintiff and other visitors’ browsers, stored on their devices, and transmitted to the Third Parties along with user data. These third-party cookies permitted the Third Parties to track and collect data in real time regarding Website visitors’ behaviors and communications, including their browsing history, visit history, website interactions, user input data, demographic information, interests and preferences, shopping behaviors, device information, referring URLs, session information, user identifiers, and/or geolocation data.

4. The Third Parties analyze and aggregate this user data across websites and time for their own purposes and financial gain, including, creating consumer profiles containing detailed information about a consumer’s behavior, preferences, and demographics; creating audience segments based on shared traits (such as Millennials, tech enthusiasts, etc.); and performing targeted advertising and marketing analytics. Further, the Third Parties share user data and/or user profiles to unknown parties to further their financial gain.

5. This type of tracking and data sharing is exactly what the Website visitors who clicked or selected the “Reject All” button on the Websites’ cookie consent banners sought to avoid. Defendant falsely told Website users that it respected their privacy and that they could avoid tracking and data sharing when they browsed the Websites. Despite receiving notice of consumers’ express declination of consent, Defendant defied it and violated state statutes, and tort duties.

THE PARTIES

6. Plaintiff Jonathan Gabrielli is, and was at all relevant times, an individual and resident of Oakland, California. Plaintiff intends to remain in California and makes his permanent home there.

1 7. Defendant Haleon US Inc. is a Delaware corporation with its headquarters and
2 principal place of business in Warren, New Jersey.

3 **JURISDICTION AND VENUE**

4 8. This Court has jurisdiction over the subject matter of this action pursuant to 28
5 U.S.C. § 1332(d)(2). The aggregate amount in controversy exceeds \$5,000,000, exclusive of
6 interest and costs; and Plaintiff and Defendant are citizens of different states.

7 9. The injuries, damages and/or harm upon which this action is based, occurred or
8 arose out of activities engaged in by Defendant within, affecting, and emanating from, the State
9 of California. Defendant regularly conducts and/or solicits business in, engages in other
10 persistent courses of conduct in, and/or derives substantial revenue from products and services
11 provided to persons in the State of California. Defendant has engaged, and continues to engage,
12 in substantial and continuous business practices in the State of California.

13 10. Venue is proper in this District pursuant to 28 U.S.C. § 1391(b)(2) because a
14 substantial part of the events or omissions giving rise to the claims occurred in the state of
15 California, including within this District.

16 11. Plaintiff accordingly alleges that jurisdiction and venue are proper in this Court.

17 **SUBSTANTIVE ALLEGATIONS**

18 A. **Defendant Programmed the Websites to Include Third-Party Resources**
19 **that Utilize Cookie Trackers.**

20 12. Every website, including the Websites, is hosted by a server that sends and
21 receives communications in the form of HTTP requests, such as “GET” or “POST” requests, to
22 and from Internet users’ browsers. For example, when a user clicks on a hyperlink on a Website,
23 the user’s browser sends a “GET” request to the Website’s server. The GET request tells the
24 Websites server what information is being requested (e.g., the URL of the webpage being
25 requested) and instructs the Website’s server to send the information back to the user (e.g., the
26 content of the webpage being requested). When the Website server receives an HTTP request, it
27 processes that request and sends back an HTTP response. The HTTP request includes the client’s
28 IP address so that the Website server to knows where to send the HTTP response.

1 13. An IP address (Internet Protocol address) is a unique numerical label assigned to
2 each device connected to a network that uses the Internet Protocol for communication, typically
3 expressed as four sets of numbers separated by periods (e.g., 192.168.123.132 for IPv4
4 addresses). IP addresses can identify the network a device is on and the specific device within
5 that network. Public IP addresses used for internet-facing devices reveal geographical locations,
6 such as country, city, or region, through IP geolocation databases.

7 14. Defendant voluntarily integrated “third-party resources” from the Third Parties
8 into the Websites’ programming. “Third-party resources” refer to tools, content or services
9 provided by third-parties, such as analytics tools, advertising networks, or payment processors,
10 that a website developer utilizes by embedding scripts, styles, media, or application
11 programming interface (API) into the website’s code. Defendant’s use of the third-party
12 resources on the Websites is done so pursuant to agreements between Defendant and those Third
13 Parties.

14 15. The Websites cause users’ devices to store and/or transmit both first-party and
15 third-party tracking cookies. Cookies are small text files sent by a website server to a user’s web
16 browser and stored locally on the user’s device. As described below, cookies generally contain
17 a unique identifier which enables the website to recognize and differentiate individual users.
18 Cookie files are sent back to the website server along with HTTP requests, enabling the website
19 to identify the device making the requests, and to record a session showing how the user interacts
20 with the website.

21 16. First-party cookies are those that are placed on the user’s browser directly by the
22 web server with which the user is knowingly communicating (in this case, the Websites’ servers).
23 First-party cookies are used to track users when they repeatedly visit the same website.

24 17. A third-party cookie is set by a third-party domain/webserver (e.g.,
25 www.youtube.com; irxcm.com; clarity.ms, etc.). When the user’s browser loads a webpage (such
26 as a webpage of the Websites) containing embedded third-party resources, the third-parties’
27 programming scripts typically issue HTTP commands to determine whether the third-party
28

1 cookies are already stored on the user's device and to cause the user's browser to store those
2 cookies on the device if they do not yet exist. Third-party cookies include an identifier that allows
3 the third-party to recognize and differentiate individual users across websites (including the
4 Websites) and across multiple browsing sessions.

5 18. As described further below, the third-party cookies stored on and/or loaded from
6 users' devices when they interact with the Websites are transmitted to those third parties,
7 enabling them to surreptitiously track in real time and collect Website users' personal
8 information, such as their browsing activities and private communications with Defendant,
9 including the following:

- 10 • **Browsing History:** Information about the webpages a Website user visits,
11 including the URLs, titles, and keywords associated with the webpages viewed,
12 time spent on each page, and navigation patterns;
- 13 • **Visit History:** Information about the frequency and total number of visits to the
14 Websites;
- 15 • **Website Interactions:** Data on which links, buttons, or ads on the Websites that
16 a user clicks;
- 17 • **User Input Data:** The information the user entered into the Websites' form
18 fields, including search queries, the user's name, age, gender, email address,
19 location, and/or payment information;
- 20 • **Demographic Information:** Inferences about age, gender, and location based on
21 browsing habits and interactions with Websites' content;
- 22 • **Interests and Preferences:** Insights into user interests based on the types of
23 Website content viewed, products searched for, or topics engaged with;
- 24 • **Shopping Behavior:** Information about the Website products viewed or added to
25 shopping carts;
- 26 • **Device Information:** Details about the Website user's device, such as the type of
27 device (mobile, tablet, desktop), operating system, and browser type;

- 1 • **Referring URL:** Information about the website that referred the user to the
- 2 Websites;
- 3 • **Session Information:** Details about the user’s current Website browsing session,
- 4 including the exact date and time of the user’s session, the session duration and
- 5 actions taken on the Websites during that session;
- 6 • **User Identifiers:** A unique ID that is used to recognize and track a specific
- 7 Website user across different websites over time; and
- 8 • **Geolocation Data:** General location information based on the Website user’s IP
- 9 address or GPS data, if accessible.

10 (Collectively, the browsing activities and private communications listed in the bullet points
11 above shall be referred to herein as “Private Communications”).

12 19. Third-party cookies can be used for a variety of purposes, including (i) analytics
13 (e.g., tracking and analyzing visitor behavior, user engagement, and effectiveness of marketing
14 campaigns); (ii) personalization (e.g., remembering a user’s browsing history and purchase
15 preferences to enable product recommendations); (iii) advertising/targeting (e.g., delivering
16 targeted advertisements based on the user’s consumer profile (i.e., an aggregated profile of the
17 user’s behavior, preferences, and demographics); and (iv) social media integration (e.g., enabling
18 sharing of users’ activities with social media platforms). Ultimately, third-party cookies are
19 utilized to boost website performance and revenue through the collection, utilization, and
20 dissemination of user data.

21 20. Defendant specializes in consumer health care products, such as digestive health
22 (tums.com); oral health (sensodyne.com); pain relief (advil.com); vitamins, minerals, and
23 supplements (emergenc.com, caltrate.com and centrum.com); and respiratory health
24 (flonase.com and theraflu.com). Defendant owns and operates the Websites, which allow visitors
25 to receive information about its products and learn how to purchase its products. As they interact
26 with the Websites (e.g., by entering data into forms, clicking on links, and making selections),
27 Website users communicate Private Communications to Defendant, including their browsing
28

1 history, visit history, website interactions, user input data, demographic information, interests
2 and preferences, shopping behaviors, device information, referring URLs, session information,
3 user identifiers, and/or geolocation data.

4 21. Defendant chose to install or integrate the Websites with resources from the Third
5 Parties that, among other things, use cookies. Thus, when consumers visit the Websites, both
6 first-party cookies and third-party cookies are placed on their devices and/or transmitted. This is
7 caused by software code that Defendant incorporates into its Websites, or that Defendant causes
8 to be loaded. Because Defendant controls the software code of its Websites, it has complete
9 control over whether first-party and third-party cookies are placed on its users' devices and/or
10 transmitted to third parties.

11 22. Defendant explained the third-party cookies it used on the Websites as follows in
12 its Privacy Notice:

13 Our websites and mobile applications may use technology called “cookies”, web
14 beacons, pixels, and similar technologies. A cookie is a small text file that is placed
15 on your hard disk by a server. Cookies and similar technologies allow our websites
16 and mobile applications to load content, remember your preferences, keep you
17 signed into your account, save your shopping cart, and provide a more personalized
experience. They also let us generate information about website traffic and trends,
and to verify your viewing and/or receipt of communications...

18 We use third-party analytics. We use automated applications to evaluate usage of
19 our website, such as Google Analytics, a web analytics service provided by Google,
Inc. We may also use other analytic means to evaluate our websites and services.
20 We use these tools to help us improve the websites, performance and user
experiences.

21 Google Analytics uses cookies to analyze use patterns and may collect information
about your use of the website, including your IP address...

22 We show targeted ads. Our websites and mobile applications may from time to time
23 provide links to or embed third party websites or content. Our advertising partners
24 may collect information about your use of our websites and apps through cookies,
web beacons, and similar technologies to display advertisements that are tailored
25 to your interests on other websites and services...¹

26 ¹ Haleon General Privacy Notice United States (updated December 22, 2022) (current version
27 available at <https://www.privacy.haleon.com/en-us/general/general-full-text/>) (the “Privacy
28 Notice”). Defendant has subsequently updated its Privacy Notice but, based on information and
belief, this version was in effect at the time of Plaintiff’s rejection of cookies on the Tums
Website.

23. Defendant provided further information about the types of third-party cookies it used on the Websites as follows in its Privacy Preference Center:

Performance Cookies. These cookies allow us to count visits and traffic sources so we can measure and improve the performance of our site. They help us know which pages are the most and least popular and see how visitors move around the site...

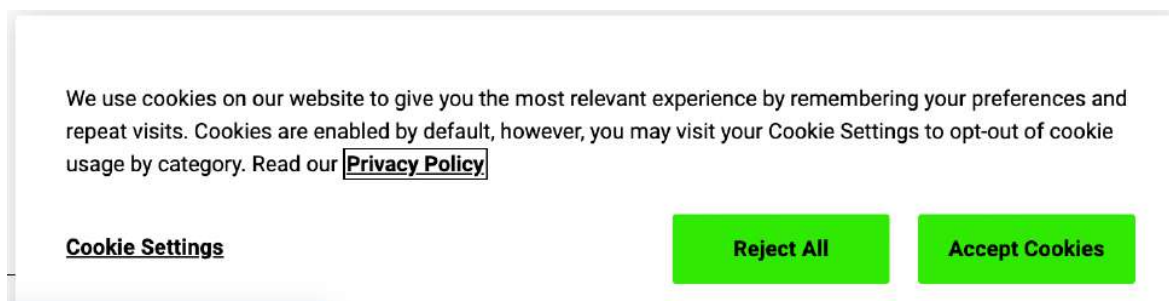
Targeting Cookies. These cookies may be set through our site by our advertising partners. They may be used by those companies to build a profile of your interests and show you relevant adverts on other sites. They do not store directly personal information, but are based on uniquely identifying your browser and internet device...

Social Media Cookies. These cookies are set by a range of social media services that we have added to the site to enable you to share our content with your friends and networks. They are capable of tracking your browser across other sites and building up a profile of your interests. They may impact the content and messages you see on other websites you visit.

Tums Website Privacy Preference Center.

B. Defendant Falsely Informed Users That They Could Reject the Websites' Use of Cookies.

24. When consumers in California visited any of the Websites, the Website immediately displayed to them a popup cookie consent banner. As shown in the screenshot below, the cookie consent banners stated, "We use cookies on our website to give you the most relevant experience by remembering your preferences and repeat visits." The banners failed to disclose that the Websites used cookies for analytics and targeted advertising functions. The Websites' banners then purported to provide users the opportunity to "Reject All" cookies as shown, in the following screenshot from the Tums Website:



1 25. The same or substantially similar cookie consent banner appeared on each of the
2 Websites.

3 26. Website users who clicked or selected the “Reject All” cookies button, indicating
4 their choice and/or agreement to decline or reject all cookies and tracking technologies in use on
5 the Websites, could then continue to browse the Websites, and the popup cookie consent banners
6 disappeared.

7 27. Defendant’s popup cookie consent banners led Plaintiff, and all those similarly
8 situated users of the Websites, to believe that they declined or rejected all cookies and tracking
9 technologies, especially those that share personal information with third parties, such as
10 performance, targeting, and social media cookies. The banners further reasonably led Plaintiff
11 and other Website users to believe that Defendant would not allow third parties, through
12 cookies, to access their Private Communications with the Websites, including their browsing
13 history, visit history, website interactions, user input data, demographic information, interests
14 and preferences, shopping behaviors, device information, referring URLs, session information,
15 user identifiers, and/or geolocation data, upon clicking or selecting the “Reject All” cookies
16 button. Defendant’s representations, however, were false.

17 28. In truth, Defendant did not abide by its users’ wishes. Even though Defendant
18 received notice that certain users, through their selection of the “Reject All” cookies button did
19 not consent to the placement or transmission of third-party cookies that would allow those
20 parties to obtain their Private Communications with the Websites, Defendant nonetheless
21 caused the Third Party tracking cookies to be placed on Website users’ browsers and devices
22 and/or transmitted to the Third Parties along with user data—even for those users who elected
23 to reject all cookies.

24 29. In particular, when users clicked or selected the “Reject All” cookies button,
25 Defendant nonetheless continued to cause the Third Parties’ cookies to be placed on users’
26 devices and/or transmitted to the Third Parties along with user data, enabling them to collect user
27 data in real time that discloses Website visitors’ Private Communications, including browsing
28

history, visit history, website interactions, user input data, demographic information, interests and preferences, shopping behaviors, device information, referring URLs, session information, user identifiers, and/or geolocation data. In other words, even when consumers like Plaintiff tried to protect their privacy by rejecting cookies, Defendant failed to prevent cookies from being transmitted to Third Parties, enabling them to track user behavior and communications.

30. Some aspects of the operations of the Third Party cookies on the Websites can be observed using specialized tools that log incoming and outgoing Website network transmissions. The following screenshots, obtained using one such tool, show examples of Third-Party cookies being transmitted from a Tums Website user's device and browser to Third Parties even after the user clicked the "Reject All" cookies button on the Tums Website's popup cookie consent banner.

The screenshot displays the Tums website interface on the left and a network log on the right. The website shows the Tums Naturals product page with two bottles of Tums Naturals (Extra Strength and Ultra 1000) and a 'Buy Now' button. The network log on the right shows various requests to third-party domains, including YouTube, irxcm.com, and cdn.userway.org, indicating that cookies are being transmitted to these third parties even after the user has rejected all cookies.

Name	Method	Status	Domain	Cookie
iframe_api	GET	200	www.youtube.com	
iframe_api	GET	200	www.youtube.com	
iframe_api	GET	200	www.youtube.com	
iframe_api	GET	200	www.youtube.com	
iframe_api	GET	200	www.youtube.com	
cpselector.jsp?parent=someld&frameid=...	GET	302	irxcm.com	
GenError.jsp?err=1101&parent=someld&f...	GET	200	irxcm.com	
iframeresizer.contenttwin.js	GET	200	irxcm.com	
imageMapResizer.min.js	GET	200	irxcm.com	
jquery.js	GET	200	irxcm.com	
imageResourceView?merchantid=28492...	GET	200	irxcm.com	
cpn?parent=someld&frameid=0&rtxuseq...	GET	200	irxcm.com	
cpn?parent=someld&rtxorigin=https%3...	GET	302	irxcm.com	
fp.min.jsp	GET	200	irxcm.com	
iframeresizer.js	GET	200	irxcm.com	
collect	POST	204	b.clarity.ms	
collect	POST	204	b.clarity.ms	
collect	POST	204	b.clarity.ms	
alts.json?dto=%7B%22sorted%22%3A%...	OPTIONS	200	cdn77.api.userway.org	
alts.json?dto=%7B%22sorted%22%3A%...	OPTIONS	200	cdn77.api.userway.org	
725034A?maxLocationsPerRetailer=10&...	OPTIONS	204	productcatalog.channeladvisor.com	
index.html?rand=1711251500760&servic...	GET	200	cdn.userway.org	
index.html?pid=12047905&model=7250...	GET	200	where-to-buy.co	
index.js?v=1711111644	GET	200	cdn.userway.org	
metropolis.css?v=1711111644	GET	200	cdn.userway.org	
logo.svg	GET	200	cdn.userway.org	

31. The screenshot above shows the “Network” tab of Chrome Developer Tools, which contains a list of HTTP network traffic transmissions between the user’s browser and various third party websites while the user visited and interacted with Defendant’s Tums Website at www.tums.com. The screenshot depicts only network traffic occurring *after* the user rejected all cookies using the cookie banner. As shown above, despite the user’s rejection of all cookies, the user’s interactions with the Tums Website caused the user’s browser to make a large number of GET and POST HTTP requests to third party web domains like www.youtube.com; irxcm.com; clarity.ms; and others. As further shown in the right-hand column of the screenshot, the user’s browser sent cookies along with those HTTP requests to the third parties. The screenshot demonstrates that the Tums Website caused third-party cookie data and users’ Private Communications to be transmitted to Third Parties, even after consumers declined or rejected all cookies and tracking technologies by clicking or selecting the “Reject All” cookies button. All of these network calls are made to the Third Parties without the user’s knowledge, and despite the user’s rejection of all cookies.

32. The other Websites similarly cause consumers’ devices to transmit user data to third parties—even after consumers *reject cookies* by clicking the “Reject All” button—on those Websites.

33. Website users’ Private Communications, including their browsing history, visit history, website interactions, user input data, demographic information, interests and preferences, shopping behaviors, device information, referring URLs, session information, user identifiers, and/or geolocation data, are surreptitiously obtained by the Third Parties via these cookies.

34. As users interact with the Websites, even after clicking or selecting the “Reject All” cookies button, thereby declining or rejecting the use of cookies and similar technologies that share personal information with third parties, such as performance, targeting, and social media cookies, more data regarding users’ behavior and communications are sent to third parties, alongside the cookie data. The third-party cookies that Defendant wrongfully allows to be stored

on users' devices and browsers, and to be transmitted to the Third Parties, enable the Third Parties to track and collect data on users' behaviors and communications, including Private Communications, on the Websites. Because third-party cookies enable Third Parties to track users' behavior across the Internet and across time, user data can be correlated and combined with other data sets to compile comprehensive user profiles that reflect consumers' behavior, preferences, and demographics (including psychological trends, predispositions, attitudes, intelligence, abilities, and aptitudes). These Third Parties monetize user profiles for advertising, sales, and marketing purposes to generate revenue and target advertising to Internet users. Advertisers can gain deep understanding of users' behavioral traits and characteristics and target those users with advertisements tailored to their consumer profiles and audience segments.

35. The Third Party code that the Websites cause to be loaded and executed by the user's browser becomes a wiretap when it is executed because it enables the Third Parties—separate and distinct entities from the parties to the conversations—to use cookies to eavesdrop upon, record, extract data from, and analyze conversations to which they are not parties. When the Third Parties use their respective wiretaps on Website users' Private Communications, the wiretaps are not like tape recorders or “tools” used by one party to record the other. The Third Parties each have the capability to use the contents of conversations they collect through their respective wiretaps for their own purposes as described in more detail below.

C. The Private Communications Collected As a Result of Third Party Cookies Transmitted When Visiting Defendant's Websites.

1. Google YouTube Cookies

36. Defendant causes third party cookies to be transmitted to and from Website users' browsers and devices, even after users reject all cookies (including advertising and analytics cookies) to and from the www.youtube.com domain, and other Google domains. Defendant currently identifies cookies from the www.youtube.com domain as “Advertising” cookies in the Tums Website Privacy Preference Center. This domain is associated with Google's YouTube, a video sharing and streaming platform which allows users to upload, watch, share, and engage

1 with video content. Google collects user information via cookies to assist it in performing data
 2 collection, behavioral analysis, user retargeting, and analytics.² Google serves targeted ads to
 3 web users across Google's ad network, which spans millions of websites, apps, and the YouTube
 4 platform. Google's cookies help it track whether users complete specific actions after interacting
 5 with an ad (e.g., clicking a link or making a purchase) and provide analytic metrics that
 6 advertisers use to measure ad campaign performance. Further, by identifying users who have
 7 shown interest in certain products or content, Google's cookies enable its advertising platform
 8 to enable advertisers to show relevant ads to those users when they visit other websites within
 9 Google's ad network.³

10 37. Google's cookies allow it to obtain and store at least the following user data:
 11 (i) browsing history, (ii) visit history, (iii) website interactions, (iv) user input data,
 12 (v) demographic information, (vi) interests and preferences, (vii) shopping behaviors,
 13 (viii) device information, (ix) referring URLs, (x) session information, (xi) user identifiers, and
 14 (xii) geolocation data.⁴

15
16
17
18 ² See Our advertising and measurement cookies (available at
<https://business.safety.google/adscookies/>).

19 ³ See, e.g. About cross-channel remarketing in Search Ads 360 (available at
<https://support.google.com/searchads/answer/7189623?hl=en>); About dynamic remarketing for
 20 retail (available at [https://support.google.com/google-
 ads/answer/6099158?hl=en&sjid=1196213575075458908-NC](https://support.google.com/google-ads/answer/6099158?hl=en&sjid=1196213575075458908-NC)).

21 ⁴ See About the Google Tag (available at
<https://support.google.com/searchads/answer/7550511?hl=en>); How Floodlight Recognizes
 22 Users (available at <https://support.google.com/searchads/answer/2903014?hl=en>); How Google
 23 Ads tracks website conversions (available at [https://support.google.com/google-
 ads/answer/7521212](https://support.google.com/google-ads/answer/7521212)); Google Ads Help, Cookie: Definition (available at
 24 <https://support.google.com/google-ads/answer/2407785?hl=en>); About demographic targeting in
 25 Google Ads (available at
[https://support.google.com/searchads/answer/7298581?hl=en&sjid=1196213575075458908-
 NC&visit_id=638670675669576522-2267083756&ref_topic=7302618&rd=1](https://support.google.com/searchads/answer/7298581?hl=en&sjid=1196213575075458908-NC&visit_id=638670675669576522-2267083756&ref_topic=7302618&rd=1)); How Google
 26 Analytics Works (<https://support.google.com/analytics/answer/12159447>); Set up events
 27 (available at <https://developers.google.com/analytics/devguides/collection/ga4/events>); and
 28 Recommended events (available at <https://support.google.com/analytics/answer/9267735>).

38. For example, the Google software code that Defendant causes to be stored on and executed by the Tums Website user's device causes the following types of cookies to be sent to Google's domain, at <https://www.youtube.com>:

Request Header Query Body Cookies Raw Summary +	
Key	Value
__Secure-3PSID	g.a000hwhMH9ivRAj5NtnWywCX4ZmM7NLM92A34W5Xsh5o-aqSaHHWfW-ocfDvc3dTsyQXwDWy5AACgYKARASQAQSFQHGx2MiEuQaYZhJlI4Yzim02AMsSRoVAUF8yKojhMzoMLiqMSvOrf8JC4Y30076
__Secure-3PAPISID	uk950RhyqIXlyJvZ/Am3N0xXU-PfcrRzBK
LOGIN_INFO	AFmmF2swRAIgYzsmi_ZLsyr4u4WT5p3S3KWGRgY90OrYQLgHjQel9XYCIB73U8WM0SgiIHG_InFsyDPuaYwuw_LKGjpiUbaxZYiw:QUQ3MjNmeTE0a2h6UC1oMGhWRk5Bd1E3Zlplc0FnSUw0clJjSllhM080dVQyNFJ3UHMzRVBaOEZ2bktrbEZsMGJ1czBiYkJYLXVknJFzRIFxV2VCZUQ5eDRZQmJ2ZEpoOHpOSVdIREFabi1rOUZDVEJBNE0Qlc5Yk1KdEh5WUxXdHMxWWN6UE1PVW9kb3VOWlpObHZPTG1ESFBSLTJIVet3
__Secure-3PSIDTS	sidts-CjEB7F1E_lRd4HNrN8-z3DXG2hna58enj7DCupgjHyaTrbWCort5o4yIc7MVeVucxvqEAA
YSC	IObTmrGA7mY
VISITOR_INFO1_LIVE	MIR80-Uj9w8
VISITOR_PRIVACY_METADATA	CgJVUxIEGgAgMg%3D%3D
__Secure-3PSIDCC	AKeyXzXV8ui8rGyZkTefEhOSWGH8Mhkxyua9NxsxAlhDuRleNIWurESewktbE0WNZjgDyL3L2o

39. At least the __Secure-3PAPISID and __Secure-3PSID cookies used on the Websites are utilized by Google to build a profile of Websites visitor interests to show relevant and personalized ads through retargeting.

40. In addition, Defendant causes the user's browser to send various first-party cookies to Google. For example, when the user browses the Tums Website—even after rejecting all cookie—Defendant causes the following cookies to be transmitted to Google:

Key	Value
_gid	GA1.2.1505092728.1711251433
_dc_gtm_UA-3967	1
8258-1	
_gat_UA-13563520	1
3-1	
_ga_PDJ657JTW7	GS1.1.1711251431.1.0.1711251431.0.0.0
_ga	GA1.1.491436158.1711251433
_ga_B1R1292CCB	GS1.1.1711251431.1.0.1711251431.0.0.0

41. The “_gid,” “_ga,” and “_ga...” cookies are associated with Google Analytics.⁵
 The “_dc_gtm” cookie is associated with Google Tag Manager.

42. Further, along with all of this data, the Google software code that Defendant causes to be stored on and executed by the user’s device causes the user’s “user-agent” information to be sent to Google:

user-agent	Mozilla/5.0 (Macintosh; Intel Mac OS X 10_15_7) AppleWebKit/537.36 (KHTML, like Gecko) Chrome/123.0.0.0 Safari/537.36
------------	---

43. The “user-agent” corresponds to the device and browser that the user has used to access the Tums Website. In this case, the user-agent value corresponds to Google’s Chrome browser version 121, running on the Catalina version of macOS.⁶

44. Finally, the data sent to Google contains the user’s IP address.

45. Because Google’s cookies operate across multiple sites (i.e., cross-site tracking), the cookie enables Google to track users as they navigate from one site to another, and to comprehensively observe and evaluate user behavior online. Google’s advertising platform

⁵ Google Resources: Our advertising and measurement cookies (available at <https://business.safety.google/adscokies/>).

⁶ There are many tools on the web that are capable of parsing user-agent strings to determine what browser and operating system they pertain to. One such tool is located at <https://explore.whatismybrowser.com/useragents/parse>.

1 aggregates user data to create consumer profiles containing detailed information about a
2 consumer's behavior, preferences, and demographics and audience segments based on shared
3 traits (such as females, Millennials, etc.), and to perform targeted advertising and marketing
4 analytics.

5 46. Thus, the Google cookies used on the Websites enable Google to track users'
6 interactions with advertisements to help advertisers understand how users engage with ads across
7 different websites. Further, the user data collected through the cookie enables the delivery of
8 personalized ads based on user interests and behaviors. For instance, if a user frequently visits
9 travel-related websites, Google will show her more travel-related advertisements. Further, the
10 collected data is used to generate reports for advertisers, helping them assess the performance of
11 their ad campaigns and make data-driven decisions (such as renaming their products). Further,
12 Google's advertising platform enables advertisers to retarget marketing, which Google explains
13 allows advertisers to "show previous visitors ads based on products or services they viewed on
14 your website. With messages tailored to your audience, dynamic remarketing helps you build
15 leads and sales by bringing previous visitors back to your website to complete what they
16 started."⁷

17 47. Further, in its "Shared Data Under Measurement Controller-Controller Data
18 Protection Terms," Google states: "Google can access and analyze the Analytics data customers
19 share with us to better understand online behavior and trends, and improve our products and
20 services—for example, to improve Google search results, detect and remove invalid advertising
21 traffic in Google Ads, and test algorithms and build models that power services like Google
22 Analytics Intelligence that apply machine-learning to surface suggestions and insights for
23 customers based on their analytics data and like Google Ads that applies broad models to
24 improve ads personalization and relevance. These capabilities are critical to the value of the
25
26

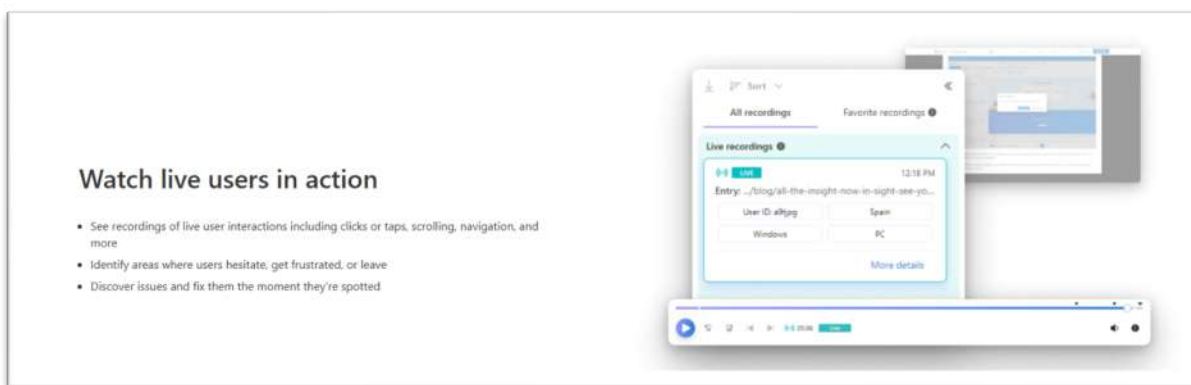
27 ⁷ Dynamic remarketing for web setup guide (available at <https://support.google.com/google-ads/answer/6077124>).
28

products we deliver to customers today.”⁸ Thus, Google can have the capability to use the data it collects for understanding online behavior and trends, machine learning, and improving its own products and services.

2. Microsoft Clarity Cookies

48. Defendant also causes third party cookies to be transmitted to and from Website users’ browsers and devices, even after users click or select the “Reject All” cookies button, to and from the clarity.ms domain. This domain is associated with Clarity, Microsoft’s “cutting-edge behavioral analytics tool that helps you understand user interaction with your website or app”.⁹ Clarity is a Microsoft Advertising tool, which “crucial for successful marketing.”¹⁰ “Clarity’s tracking code” “uses a cookie to obtain user session data.”¹¹

49. Clarity, however, allows Defendant to “watch live users in action” via “recordings of live user interactions” on the website, including a user’s “clicks or taps, scrolling, navigation, and more.”¹² Indeed, Clarity boasts that it “tracks all visitor clicks and scrolls on mobile, desktop, and tablet[.]” These “session recordings” track each and every consumer’s individual actions on the website.¹³



⁸ Shared Data Under Measurement Controller-Controller Data Protection Terms (available at <https://support.google.com/analytics/answer/9024351>).

⁹ <https://learn.microsoft.com/en-us/clarity/setup-and-installation/about-clarity>.

¹⁰ <https://about.ads.microsoft.com/en/blog/post/october-2021/introducing-microsoft-clarity-insights-for-microsoft-advertising>.

¹¹ <https://learn.microsoft.com/en-us/clarity/setup-and-installation/cookie-consent>.

¹² <https://clarity.microsoft.com/session-recordings>.

¹³ *Id.*

50. Along with this data, the Microsoft software that Defendant's Tums Website causes to be executed by users' browsers causes the MUID cookie to be sent to Microsoft:

Request	Header	Query	Body	Cookies	Raw	Summary
Key	Value					
MUID	28102054DABB6CEC1D8A341DDB136D83					

51. According to Microsoft's documentation, the "MUID" cookie "[i]dentifies unique web browsers visiting Microsoft sites [and is] used for advertising, site analytics, and other operational purposes."¹⁴

52. In addition, Defendant causes the user's browser to send various first-party cookies to Microsoft. For example, when the user browses the Tums Website—even after rejecting all cookies—Defendant causes the following cookies to be transmitted to Microsoft Clarity:

GET	200	https://www.tums.com/about-heartburn/				
Request	Header	Query	Body	Cookies	Raw	Summary
Key	Value					
_clck	bkhqrrq%7C2%7Cfkc%7C0%7C1544					
_clsk	5z11l7%7C1711251432578%7C1%7C0%7Cb.clarity.ms%2Fcollect					

53. Microsoft's documentation states that the "_clck" cookie "[p]ersists the Clarity User ID and preferences, unique to that site is attributed to the same user ID" and that the "_clsk" cookie "[c]onnects multiple page views by a user into a single Clarity session recording."¹⁵

54. Further, Clarity permits Defendant to aggregate individual users' session recordings into "heatmaps" for Defendant's financial gain. Heatmaps are "visualization tool[s]" aimed at "aggregat[ing] information about how users interact with the website."¹⁶ This allows

¹⁴ <https://learn.microsoft.com/en-us/clarity/setup-and-installation/cookie-list>.

¹⁵ *Id.*

¹⁶ <https://learn.microsoft.com/en-us/clarity/heatmaps/heatmaps-overview>.

Defendant to “See at a glance which areas on [web site owner’s] page drive the most engagement,” a crucial element to increasing advertising revenue.¹⁷ Clarity also permits Defendant to “track a specific subset of users,” including tracking metrics like what browser users visited from, what type of device, the date, and more. Clarity even permits the use of specific “Clarity user ID[s]” which permits Clarity to track users across their devices, and identify when the same user visits multiple times to the website.¹⁸ Businesses use Clarity to “make data-driven decisions” to “improve overall conversion rates” of clicks, engagement, or sales.¹⁹ Microsoft notes in a Clarity case study that Clarity cookies permitted businesses to see a “substantial increase” in “purchases.”²⁰ In one instance, “following just five days after implementing Clarity, the [business] saw an uplift of 19% in conversion rate.”²¹ Businesses consider Clarity a “must-have tool for any business serious about optimizing their website and increasing online revenue.”²²

55. Microsoft collects data from Clarity,²³ which “Microsoft retains . . . for as long as necessary[.]”²⁴ Clarity cookies allow Microsoft to obtain and store at least the following user data: (i) user identifier; (ii) website interactions; (iii) interests and preferences; (iv) shopping behavior; (v) device information; (vi) demographic data; (vii) geolocation data; (viii) referring URL; and (ix) session information.²⁵

¹⁷ <https://clarity.microsoft.com/heatmaps>.

¹⁸ <https://clarity.microsoft.com/insights>; <https://learn.microsoft.com/en-us/clarity/setup-and-installation/identify-api>.

¹⁹ <https://clarity.microsoft.com/case-studies/ecommerce-boost/#:~:text=Using%20Clarity&text=By%20analyzing%20user%20sessions%20and,and%20improve%20overall%20conversion%20rates>.

²⁰ *Id.*

²¹ *Id.*, emphasis in original.

²² <https://clarity.microsoft.com/case-studies/ecommerce-boost/#:~:text=Using%20Clarity&text=By%20analyzing%20user%20sessions%20and,and%20improve%20overall%20conversion%20rates>.

²³ <https://www.microsoft.com/en-us/privacy/privacystatement>.

²⁴ *Id.*

²⁵ <https://learn.microsoft.com/en-us/clarity/setup-and-installation/clarity-data>.

3. RevTrax Cookies

56. Defendant also causes third party cookies to be transmitted to and from Website users' browsers and devices, even after users click or select the "Reject All" cookies button, to and from the irxcm.com domain. This domain is associated with RevTrax, a digital service provided by Neptune Retail Solutions that allows website owners to offer digital coupons and offers to customers.²⁶ "The RevTrax Technology presents a Client's Web-based offer to a User using the RevTrax-owned website irxcm.com, and collects Usage Data and Tracking Data" which Neptune explains includes "a User's device type, operating system version, and Internet browser type and version" and "IP address" (Usage Data) and "information collected by the RevTrax Technology from a User who is presented with a Web-based offer" (Tracking Data) that includes data about how the user interacts with the offer and the user's email address or phone number (if provided).²⁷ RevTrax cookies allow Neptune to obtain and store at least the following user data: (i) user identifier; (ii) website interactions; (iii) shopping behavior; (iv) device information; (v) geolocation data; and (vi) session information.²⁸

57. The RevTrax Technology utilizes the user data to "[p]repare reports and analytics, and perform other services, as requested by [website owners]" and "identify[] usage trends, diagnosing technical problems, operating, maintaining, enhancing and improving the RevTrax Technology and RevTrax Service, and developing new products and services."²⁹

D. The Private Communications Collected are Valuable.

58. The Private Communications that the Third Parties track and collect by way of the cookies on the Websites is valuable to Defendant as well as the Third Parties. Defendant can use the data to create and analyze the performance of marketing campaigns, website design, product placement, and target specific users or groups of users for advertisements. For instance,

²⁶ <https://www.revtrax.com/privacy-policy>.

²⁷ *Id.*

²⁸ <https://learn.microsoft.com/en-us/clarity/setup-and-installation/clarity-data>.

²⁹ *Id.*

1 if Defendant wanted to market certain of its products to consumers, Defendant could use the data
2 collected by the Third Parties to monitor users who visit webpages related to specific products,
3 then advertise similar products to those particular users when they visit other webpages. The
4 third-party cookies also enable Defendant to target online advertisements to users when they
5 visit *other* websites, even those completely unrelated to Defendant and its products.

6 59. Data about users' browsing history enables Defendant to spot patterns in users'
7 behavior on the Websites and their interests in, among other things, Defendant's products. On a
8 broader scale, it enables Defendant to gain an understanding of trends happening across its
9 brands and across the consumer electronics market. All of this helps Defendant further monetize
10 its Websites and maximize revenue by collecting and analyzing user data.

11 60. The value of the Private Communications tracked and collected by the Third
12 Parties using cookies on the Websites can be quantified. Legal scholars observe that "[p]ersonal
13 information is an important currency in the new millennium."³⁰ Indeed, "[t]he monetary value
14 of personal data is large and still growing, and corporate America is moving quickly to profit
15 from the trend." *Id.* "Companies view this information as a corporate asset and have invested
16 heavily in software that facilitates the collection of consumer information." *Id.*

17 61. Numerous empirical studies quantify the appropriate value measure for personal
18 data. Generally, the value of personal data is measured as either the consumer's willingness to
19 accept compensation to sell her data or the consumer's willingness to pay to protect her
20 information.

21 62. Through its false representations and aiding, agreeing with, employing,
22 permitting, or otherwise enabling the Third Parties to track users' Private Communications on
23 the Website using third-party cookies, Defendant is unjustly enriching itself at the cost of
24 consumer privacy and choice, when the consumer could otherwise have the ability to choose if
25 and how they would monetize their data.

26
27
28 ³⁰ See Paul M. Schwartz, *Property, Privacy and Personal Data*, 117 Harv. L. Rev. 2055, 2056–
57 (2004).

PLAINTIFF'S EXPERIENCES

63. Plaintiff visited the Tums Website to browse information about the Tums products on or around August 2023. Plaintiff visited the Emergenc Website to browse information about the Emergenc products on or around January 2024. Plaintiff visited the Centrum Website to browse information about the Centrum products on or around November 2023. Plaintiff visited the Sensodyne Website to browse information about the Sensodyne products on or around June 2024.

64. When Plaintiff visited the Websites, the Websites immediately presented him with Defendant's popup cookie consent banner, which provided the option to select the "Reject All" cookies button. Plaintiff viewed Defendant's representation on the popup cookie consent banner that, "We use cookies on our website to give you the most relevant experience by remembering your preferences and repeat visits." Plaintiff also viewed Defendant's additional representation that users could "Reject All" cookies.

65. Consistent with his typical practice in rejecting or otherwise declining the placement or use of cookies and tracking technologies, Plaintiff selected and clicked the "Reject All" cookies button. Plaintiff believed that selecting the "Reject All" cookies button on the popup cookie consent banner found on the Websites would allow him to opt out of, decline, and/or reject all cookies and other tracking technologies (inclusive of those cookies that cause the disclosure of user data to third-party advertising networks, analytics services, and/or social media companies for the purposes of providing personalized content, advertising, and analytics services).

66. In selecting the "Reject All" cookies button Plaintiff gave Defendant notice that he did not consent to the use or placement of cookies and tracking technologies while browsing the Websites. In reliance on these representations and promises, only then did Plaintiff continue browsing the Websites.

67. Even before the popup cookie consent banner appeared on the screen, Defendant nonetheless caused cookies and tracking technologies, including those used for performance,

1 targeting, and social media functions, to be placed on Plaintiff's device and/or transmitted to the
2 Third Parties along with user data, without Plaintiff's knowledge. Accordingly, the popup cookie
3 consent banner's representation to Plaintiff that he could reject the use and/or placement of all
4 cookies and tracking technologies while he browsed the Websites was false. Contrary to what
5 Defendant made Plaintiff believe, he did not have a choice about whether third-party cookies
6 would be placed on his device and/or transmitted to the Third Parties along with his user data;
7 rather, Defendant had already caused that to happen.

8 68. Then, as Plaintiff continued to browse the Websites in reliance on the promises
9 Defendant made in the cookie consent banner, and despite Plaintiff's clear rejection of the use
10 and/or placement of such cookies and tracking technologies, Defendant nonetheless continued
11 to cause the placement and/or transmission of cookies along with user data, including those
12 involved in providing performance, targeting, and social media services, from the Third Parties
13 on his device. In doing so, Defendant permitted the Third Parties to track and collect Plaintiff's
14 Private Communications as Plaintiff browsed the Websites.

15 69. Defendant's representations that consumers could "Reject All" cookies while
16 Plaintiff and users browsed the Websites were untrue. Had Plaintiff known this fact, he would
17 not have used the Websites. Moreover, Plaintiff reviewed the popup cookie consent banner prior
18 to using the Websites. Had Defendant disclosed that it would continue to cause cookies and
19 tracking technologies to be stored on consumers' devices even after they choose to reject all
20 cookies, Plaintiff would have noticed it and would not have used the Websites or, at a minimum,
21 he would have interacted with the Websites differently.

22 70. Plaintiff continues to desire to browse content featured on the Websites. Plaintiff
23 would like to browse websites that do not misrepresent that users can reject all cookies and
24 tracking technologies. If the Websites were programmed to honor users' requests to reject
25 cookies and tracking technologies, Plaintiff would likely browse the Websites again in the future,
26 but will not do so until then. Plaintiff regularly visits websites that feature content similar to that
27 of the Websites. Because Plaintiff does not know how the Websites are programmed, which can
28

1 change over time, and because he does not have the technical knowledge necessary to test
2 whether the Websites honors users' requests to reject all cookies and tracking technologies,
3 Plaintiff will be unable to rely on Defendant's representations when browsing the Websites in
4 the future absent an injunction that prohibits Defendant from making misrepresentations on the
5 Websites. The only way to determine what network traffic is sent to third parties when visiting
6 a website is to use a specialized tool such as Chrome Developer Tools. As the name suggests,
7 such tools are designed for use by "developers" (i.e., software developers), whose specialized
8 training enables them to analyze the data underlying the HTTP traffic to determine what data, if
9 any, is being sent to whom. Plaintiff is not a software developer and has not received training
10 with respect to HTTP network calls.

11 TOLLING

12 71. All applicable statutes of limitations have been tolled by operation of the delayed
13 discovery doctrine, which delays accrual until Plaintiff has, or should have, inquiry notice of his
14 causes of action. Despite exercising reasonable diligence, Plaintiff was unaware of Defendant's
15 fraudulent and unlawful conduct alleged herein due to Defendant's active concealment of
16 material facts, which prevented Plaintiff from discovering his claims within the statute of
17 limitations. As alleged above, Plaintiff does not have the expertise to test whether the Websites
18 honored users' requests to opt out of cookies and tracking technologies. Plaintiff was unaware
19 that even though he rejected cookies on the Tums Website, Defendant caused cookies, including
20 the Third Parties' cookies, to be sent to his browsers, stored on his devices, and transmitted to
21 the Third Parties along with his private user data until on or around February 2024 when he
22 learned of Defendant's privacy violations from counsel.

23 72. On or around March 25, 2024, Plaintiff notified Defendant of his claims and
24 allegations asserted herein. On February 7, 2025, the parties entered into a tolling agreement that
25 "Any and all statute of limitations periods and statute of repose periods related to Claimant's
26 alleged claims for damages and other relief against Haleon shall be tolled during the time period
27 commencing on February 7, 2025, and continuing until March 10, 2025."
28

73. Defendant has not been prejudiced in its ability to gather evidence for Plaintiff's claims since the claims asserted herein are substantially similar to those raised in Plaintiff's March 25, 2024 letter.

CLASS ALLEGATIONS

74. Plaintiff brings this Class Action Complaint on behalf of himself and a proposed class of similarly situated persons, pursuant to Rules 23(b)(2) and (b)(3) of the Federal Rules of Civil Procedure. Plaintiff seeks to represent the following group of similarly situated persons, defined as follows:

Class: All persons who browsed any of the Websites in the State of California after clicking the "Reject All" cookies button in the Website's popup cookies consent banner within the four years preceding the filing of this Complaint (the "Class Period").

75. This action has been brought and may properly be maintained as a class action against Defendant because there is a well-defined community of interest in the litigation and the proposed class is easily ascertainable.

76. **Numerosity:** Plaintiff does not know the exact size of the Class, but he estimates that it is composed of more than 100 persons. The persons in the Class are so numerous that the joinder of all such persons is impracticable and the disposition of their claims in a class action rather than in individual actions will benefit the parties and the courts.

77. **Common Questions Predominate:** This action involves common questions of law and fact to the Class because each class member's claim derives from the same unlawful conduct that led them to believe that Defendant would not cause third-party cookies to be placed on their browsers and devices and/or transmitted to third parties along with user data, after Class members chose to reject all cookies and tracking technologies on the Websites, nor would Defendant permit third parties to track and collect Class members' Private Communications as Class members browsed the Websites.

1 78. The common questions of law and fact predominate over individual questions, as
2 proof of a common or single set of facts will establish the right of each member of the Class to
3 recover. The questions of law and fact common to the Class are:

- 4 a. Whether Defendant's actions violate California laws invoked herein; and
5 b. Whether Plaintiff and Class members are entitled to damages, restitution,
6 injunctive and other equitable relief, reasonable attorneys' fees, prejudgment interest and costs
7 of this suit.

8 79. **Typicality:** Plaintiff's claims are typical of the claims of the other members of
9 the Class because, among other things, Plaintiff, like the other Class members, visited the
10 Websites, rejected all cookies, and had his confidential Private Communications intercepted by
11 the Third Parties.

12 80. **Adequacy of Representation:** Plaintiff will fairly and adequately protect the
13 interests of all Class members because it is in his best interests to prosecute the claims alleged
14 herein to obtain full compensation due to him for the unfair and illegal conduct of which he
15 complains. Plaintiff also has no interests in conflict with, or antagonistic to, the interests of Class
16 members. Plaintiff has retained highly competent and experienced class action attorneys to
17 represent his interests and those of the Class. By prevailing on his claims, Plaintiff will establish
18 Defendant's liability to all Class members. Plaintiff and his counsel have the necessary financial
19 resources to adequately and vigorously litigate this class action, and Plaintiff and counsel are
20 aware of their fiduciary responsibilities to the Class members and are determined to diligently
21 discharge those duties by vigorously seeking the maximum possible recovery for Class members.

22 81. **Superiority:** There is no plain, speedy, or adequate remedy other than by
23 maintenance of this class action. The prosecution of individual remedies by members of the Class
24 will tend to establish inconsistent standards of conduct for Defendant and result in the
25 impairment of Class members' rights and the disposition of their interests through actions to
26 which they were not parties. Class action treatment will permit a large number of similarly
27
28

1 situated persons to prosecute their common claims in a single forum simultaneously, efficiently,
 2 and without the unnecessary duplication of effort and expense that numerous individual actions
 3 would engender. Furthermore, as the damages suffered by each individual member of the Class
 4 may be relatively small, the expenses and burden of individual litigation would make it difficult
 5 or impossible for individual members of the class to redress the wrongs done to them, while an
 6 important public interest will be served by addressing the matter as a class action. Plaintiff is
 7 unaware of any difficulties that are likely to be encountered in the management of this action
 8 that would preclude its maintenance as a class action.

9 **CAUSES OF ACTION**

10 **First Cause of Action: Invasion of Privacy**

11
 12 82. Plaintiff realleges and incorporates the paragraphs of this Complaint as if set forth
 13 herein.

14 83. To plead an invasion of privacy claim, Plaintiff must show an invasion of (i) a
 15 legally protected privacy interest; (ii) where Plaintiff had a reasonable expectation of privacy in
 16 the circumstances; and (iii) conduct by Defendant constituting a serious invasion of privacy.

17 84. Defendant has intruded upon the following legally protected privacy interests of
 18 Plaintiff and Class members: (i) the California Invasion of Privacy Act, as alleged herein; (ii) the
 19 California Constitution, which guarantees Californians the right to privacy; (iii) the California
 20 Wiretap Acts as alleged herein; (iv) Cal. Penal Code § 484(a), which prohibits the knowing theft
 21 or defrauding of property “by any false or fraudulent representation or pretense;” and
 22 (v) Plaintiff’s and Class members’ Fourth Amendment right to privacy.

23 85. Plaintiff and Class members had a reasonable expectation of privacy under the
 24 circumstances, as Defendant affirmatively promised users they could “Reject All” cookies and
 25 tracking technologies before proceeding to browse the Websites. Plaintiff and other Class
 26 members directed their electronic devices to access the Websites and, when presented with the
 27 popup cookies consent banners on the Websites, Plaintiff and Class members rejected all cookies
 28 and reasonably expected that his and their rejection of all cookies and tracking technologies

1 would be honored. That is, he and they reasonably believed that Defendant would not permit the
2 Third Parties to store and send cookies and/or use other such tracking technologies on their
3 devices while they browsed the Websites. Plaintiff and Class members also reasonably expected
4 that, if they rejected all cookies and/or tracking technologies, Defendant would not permit the
5 Third Parties to track and collect Plaintiff's and Class members' Private Communications,
6 including their browsing history, visit history, website interactions, user input data, demographic
7 information, interests and preferences, shopping behaviors, device information, referring URLs,
8 session information, user identifiers, and/or geolocation data, on the Websites.

9 86. Such information is "personal information" under California law, which defines
10 personal information as including "Internet or other electronic network activity information,"
11 such as "browsing history, search history, and information regarding a consumer's interaction
12 with an internet website, application, or advertisement." Cal. Civ. Code § 1798.140.

13 87. Defendant, in violation of Plaintiff's and other Class members' reasonable
14 expectation of privacy, and without their consent, permits the Third Parties to use cookies and
15 other tracking technologies to collect, track, and compile users' Private Communications,
16 including their browsing history, visit history, website interactions, user input data, demographic
17 information, interests and preferences, shopping behaviors, device information, referring URLs,
18 session information, user identifiers, and/or geolocation data. The data that Defendant allowed
19 third parties to collect enables the Third Parties to, *inter alia*, create consumer profiles containing
20 detailed information about a consumer's behavior, preferences, and demographics; create
21 audience segments based on shared traits (such as millennials, tech enthusiasts, etc.); and
22 perform targeted advertising and marketing analytics. Further, the Third Parties share user data
23 and/or the user profiles to unknown parties to further their financial gain. The consumer profiles
24 are and can be used to further invade Plaintiff's and users' privacy, by allowing third parties to
25 learn intimate details of their lives, and target them for advertising and other purposes, as
26 described herein, thereby harming them through the abrogation of their autonomy and their
27 ability to control dissemination and use of information about them.

88. Defendant's actions constituted a serious invasion of privacy in that it invaded a zone of privacy protected by the Fourth Amendment (i.e., one's personal communications), and violated criminal laws on wiretapping and invasion of privacy. These acts constitute an egregious breach of social norms that is highly offensive.

89. Defendant's intrusion into Plaintiff's privacy was also highly offensive to a reasonable person.

90. Defendant lacked a legitimate business interest in causing the placement and/or transmission of third-party cookies along with user data that allowed the Third Parties to track, intercept, receive, and collect Private Communications, including their browsing history, visit history, website interactions, user input data, demographic information, interests and preferences, shopping behaviors, device information, referring URLs, session information, user identifiers, and/or geolocation data, without their consent.

91. Plaintiff and Class members have been damaged by Defendant's invasion of their privacy and are entitled to just compensation, including monetary damages.

92. Plaintiff and Class members seeks appropriate relief for that injury, including but not limited to, damages that will compensate them for the harm to their privacy interests as well as disgorgement of profits made by Defendant as a result of its intrusions upon Plaintiff's and Class members' privacy.

93. Plaintiff and Class members seek punitive damages because Defendant's actions—which were malicious, oppressive, willful—were calculated to injure Plaintiff and Class members and made in conscious disregard of Plaintiff's and Class members' rights and Plaintiff's and Class members' rejection of the Website's use of all cookies. Punitive damages are warranted to deter Defendant from engaging in future misconduct.

Second Cause of Action: Intrusion Upon Seclusion

94. Plaintiff realleges and incorporates by reference all paragraphs alleged herein.

95. To assert a claim for intrusion upon seclusion, Plaintiff must plead (i) that Defendant intentionally intruded into a place, conversation, or matter as to which Plaintiff had a

1 reasonable expectation of privacy; and (ii) that the intrusion was highly offensive to a reasonable
2 person.

3 96. By permitting third-party cookies to be stored on consumers' devices, which
4 enabled the Third Parties to track and collect Plaintiff's and Class members' Private
5 Communications, including their browsing history, visit history, website interactions, user input
6 data, demographic information, interests and preferences, shopping behaviors, device
7 information, referring URLs, session information, user identifiers, and/or geolocation data, in
8 violation of Defendant's representations otherwise in the Websites' popup cookie consent
9 banners, Defendant intentionally intruded upon the solitude or seclusion of Website users.
10 Defendant effectively placed the Third Parties in the middle of communications to which they
11 were not invited, welcomed, or authorized.

12 97. The Third Parties' tracking and collecting of Plaintiff's and Class member's
13 Private Communications on the Websites using third-party cookies that Defendant caused to be
14 stored on users' devices—and to be transmitted to Third Parties—was not authorized by Plaintiff
15 and Class members, and, in fact, those Website users specifically chose to "Reject All" cookies.

16 98. Plaintiff and the Class members had an objectively reasonable expectation of
17 privacy surrounding his and their Private Communications on the Websites based on Defendant's
18 promise that users could "Reject All" cookies, as well as state criminal and civil laws designed
19 to protect individual privacy.

20 99. Defendant's intentional intrusion into Plaintiff's and other Website users' Private
21 Communications would be highly offensive to a reasonable person given that Defendant
22 represented that Website users could "Reject All" cookies when, in fact, Defendant caused such
23 third-party cookies to be stored on consumers' devices and browsers, and to be transmitted to
24 third parties, even when consumers rejected all such cookies. Indeed, Plaintiff and Class
25 members reasonably expected, based on Defendant's false representations, that when he and they
26 rejected all cookies and tracking technologies, Defendant would not cause such third-party
27 cookies to be stored on his and their devices or permit the Third Parties to obtain their Private
28

1 Communications on the Websites, including their browsing history, visit history, website
 2 interactions, user input data, demographic information, interests and preferences, shopping
 3 behaviors, device information, referring URLs, session information, user identifiers, and/or
 4 geolocation data.

5 100. Defendant's conduct was intentional and intruded on Plaintiff's and users' Private
 6 Communications on the Websites.

7 101. Plaintiff and Class members have been damaged by Defendant's invasion of their
 8 privacy and are entitled to just compensation, including monetary damages.

9 102. Plaintiff and Class members seeks appropriate relief for that injury, including but
 10 not limited to, damages that will compensate them for the harm to their privacy interests as well
 11 as disgorgement of profits made by Defendant as a result of its intrusions upon Plaintiff's and
 12 Class members' privacy.

13 103. Plaintiff and Class members seek punitive damages because Defendant's
 14 actions—which were malicious, oppressive, willful—were calculated to injure Plaintiff and
 15 Class members and made in conscious disregard of Plaintiff's and Class members' rights and
 16 Plaintiff's and Class members' rejection of the Website's use of cookies. Punitive damages are
 17 warranted to deter Defendant from engaging in future misconduct.

18 **Third Cause of Action: Wiretapping in Violation of the California Invasion of Privacy**
 19 **Act (California Penal Code § 631)**

20 104. Plaintiff realleges and incorporates by reference all paragraphs alleged herein.

21 105. California Penal Code § 631(a) provides, in pertinent part:

22 “Any person who, by means of any machine, instrument, or contrivance, or in
 23 any other manner . . . willfully and without the consent of all parties to the
 24 communication, or in any unauthorized manner, reads, or attempts to read, or to
 25 learn the contents or meaning of any message, report, or communication while
 26 the same is in transit or passing over any wire, line, or cable, or is being sent from,
 27 or received at any place within this state; or who uses, or attempts to use, in any
 28 manner, or for any purpose, or to communicate in any way, any information so
 obtained, or who aids, agrees with, employs, or conspires with any person or
 persons to unlawfully do, or permit, or cause to be done any of the acts or things
 mentioned above in this section, is punishable by a fine not exceeding two
 thousand five hundred dollars”

106. The California Supreme Court has repeatedly stated an “express objective” of CIPA is to “protect a person placing or receiving a call from a situation where the person on the other end of the line permits an outsider to tap his telephone or listen in on the call.” *Ribas v. Clark*, 38 Cal. 3d 355, 364 (1985) (emphasis added).

107. Further, as the California Supreme Court has held, in explaining the legislative purpose behind CIPA:

While one who imparts private information risks the betrayal of his confidence by the other party, a substantial distinction has been recognized between the secondhand repetition of the contents of a conversation and *its simultaneous dissemination to an unannounced second auditor, whether that auditor be a person or mechanical device*.

As one commentator has noted, such secret monitoring denies the speaker an important aspect of privacy of communication—the right to control the nature and extent of the firsthand dissemination of his statements.

Ribas, 38 Cal. 3d at 360-61 (emphasis supplied; internal citations omitted).

108. CIPA § 631(a) imposes liability for “distinct and mutually independent patterns of conduct.” *Tavernetti v. Superior Ct.*, 22 Cal. 3d 187, 192-93 (1978). Thus, to establish liability under § 631(a), Plaintiff need only establish that Defendant, “by means of any machine, instrument, contrivance, or in any other manner,” did **any** of the following:

[i] Intentionally taps, or makes any unauthorized connection, whether physically, electrically, acoustically, inductively or otherwise, with any telegraph or telephone wire, line, cable, or instrument, including the wire, line, cable, or instrument of any internal telephonic communication system;

[ii] Willfully and without the consent of all parties to the communication, or in any unauthorized manner, reads or attempts to read or learn the contents or meaning of any message, report, or communication while the same is in transit or passing over any wire, line or cable or is being sent from or received at any place within this state;

[iii] Uses, or attempts to use, in any manner, or for any purpose, or to communicate in any way, any information so obtained

Cal. Penal Code § 631(a).

109. CIPA § 631(a) also penalizes those who [iv] “aid[], agree[] with, employ[], or conspire[] with any person” who conducts the aforementioned wiretapping, or those who “permit” the wiretapping.

110. Defendant is a “person” within the meaning of California Penal Code § 631.

111. Section 631(a) is not limited to phone lines, but also applies to “new technologies” such as computers, the Internet, and email. *See Matera v. Google Inc.*, 2016 WL 8200619, at *21 (N.D. Cal. Aug. 12, 2016) (CIPA applies to “new technologies” and must be construed broadly to effectuate its remedial purpose of protecting privacy); *see also Bradley v. Google, Inc.*, 2006 WL 3798134, at *5–6 (N.D. Cal. Dec. 22, 2006) (CIPA governs “electronic communications”); *Javier v. Assurance IQ, LLC*, 2022 WL 1744107, at *1 (9th Cir. May 31, 2022) (“Though written in terms of wiretapping, Section 631(a) applies to Internet communications.”).

112. The Third Parties’ cookies—as well as the software code of the Third Parties responsible for placing the cookies and transmitting data from user devices to the Third Parties—constitute “machine[s], instrument[s], or contrivance[s]” under the CIPA (and, even if they do not, Defendant’s deliberate and purposeful scheme that facilitated the interceptions falls under the broad statutory catch-all category of “any other manner”).

113. Each of the Third Parties is a “separate legal entity that offers [a] ‘software-as-a-service’ and not merely a passive device.” *Saleh v. Nike, Inc.*, 562 F. Supp. 3d 503, 520 (C.D. Cal. 2021). Further, the Third Parties had the capability to use the wiretapped information for their own purposes and, as alleged above, they did in fact use the wiretapped information for their own business purposes.

114. Under § 631(a), Defendant must show it had the consent of all parties to a communication.

115. At all relevant times, the Websites caused Plaintiff and Class members’ browsers to store the Third Parties’ cookies and to transmit those cookies alongside Private Communications—including their browsing history, visit history, website interactions, user input data, demographic information, interests and preferences, shopping behaviors, device information, referring URLs, session information, user identifiers, and/or geolocation data—to the Third Parties without Plaintiff’s and Class members’ consent. By configuring the Websites

1 in this manner, Defendant willfully aided, agreed with, employed, permitted, or otherwise
2 enabled the Third Parties to wiretap Plaintiff and Class members using the Third Parties' cookies
3 and to accomplish the wrongful conduct alleged herein.

4 116. At all relevant times, by their cookies and corresponding software code, the Third
5 Parties willfully and without the consent of all parties to the communication, or in any
6 unauthorized manner, read, attempted to read, and/or learned the contents or meaning of
7 electronic communications of Plaintiff and Class members, on the one hand, and Defendant, on
8 the other, while the electronic communications were in transit or were being sent from or
9 received at any place within California.

10 117. The Private Communications of Plaintiff and Class members, on the one hand,
11 and Defendant, on the other, that the Third Parties automatically intercepted directly
12 communicates the Website user's affirmative decisions, actions, choices, preferences, and
13 activities, which constitute the "contents" of electronic communications, including their
14 browsing history, visit history, website interactions, user input data, demographic information,
15 interests and preferences, shopping behaviors, device information, referring URLs, session
16 information, user identifiers, and/or geolocation data.

17 118. At all relevant times, the Third Parties used or attempted to use the Private
18 Communications automatically intercepted by their cookie tracking technologies for their own
19 purposes.

20 119. Plaintiff and Class members did not provide their prior consent to the Third
21 Parties' intentional access, interception, reading, learning, recording, collection, and usage of
22 Plaintiff's and Class members' electronic communications. Nor did Plaintiff and Class members
23 provide their prior consent to Defendant aiding, agreeing with, employing, permitting, or
24 otherwise enabling the Third Parties' conduct. On the contrary, Plaintiff and Class members
25 expressly declined to allow Third Parties' cookies and tracking technologies to access, intercept,
26 read, learn, record, collect, and use Plaintiff's and Class members' electronic communications
27 by choosing "Reject All" cookies in the Websites' cookie consent banners.

1 120. The wiretapping of Plaintiff and Class members occurred in California, where
2 Plaintiff and Class members accessed the Websites and where the Third Parties—as enabled by
3 Defendant—routed Plaintiff’s and Class members’ electronic communications to Third Parties’
4 servers. Among other things, the cookies, as well as the software code responsible for placing
5 the cookies and transmitting them and other Private Communications to the Third Parties, resided
6 on Plaintiff’s California-located device. In particular, the user’s California-based device, after
7 downloading the software code from the Third Parties’ servers, (i) stored the code onto the user’s
8 disk; (ii) converted the code into machine-executable format; and (iii) executed the code, causing
9 the transmission of data (including cookie data) to and from the Third Parties.

10 121. Plaintiff and Class members have suffered loss by reason of these violations,
11 including, but not limited to, (i) violation of his and their right to privacy; (ii) loss of value in
12 [his] and their Private Communications; (iii) damage to and loss of Plaintiff’s and Class
13 members’ property right to control the dissemination and use of their Private Communications;
14 and (iv) loss of their Private Communications to the Third Parties with no consent.

15 122. Pursuant to California Penal Code § 637.2, Plaintiff and Class members have been
16 injured by the violations of California Penal Code § 631, and each seeks statutory damages of
17 the greater of \$5,000, or three times the amount of actual damages, for each of Defendant’s
18 violations of CIPA § 631(a), as well as injunctive relief.

19 123. Unless enjoined, Defendant will continue to commit the illegal acts alleged herein
20 including, but not limited to, permitting third parties to access, intercept, read, learn, record,
21 collect, and use Plaintiff’s and Class members’ electronic Private Communications with
22 Defendant. Plaintiff, Class members, and the general public continue to be at risk because
23 Plaintiff, Class members, and the general public frequently use the internet to search for
24 information and content related to consumer health care products. Plaintiff, Class members, and
25 the general public continue to desire to use the internet for that purpose. Plaintiff, Class members,
26 and the general public have no practical way to know if his and their request to reject all cookies
27 and tracking technologies will be honored and/or whether Defendant will permit third parties to
28

access, intercept, read, learn, record, collect, and use Plaintiff's and Class members' electronic Private Communications with Defendant. Further, Defendant has already permitted the Third Parties to access, intercept, read, learn, record, collect, and use Plaintiff's and Class members' electronic Private Communications with Defendant and will continue to do so unless and until enjoined.

Fourth Cause of Action: Use of a Pen Register in Violation of the California Invasion of Privacy Act (California Penal Code § 638.51)

124. Plaintiff realleges and incorporates by reference all paragraphs alleged herein.

125. The California Invasion of Privacy Act, codified at Cal. Penal Code §§ 630 to 638, includes the following statement of purpose:

The Legislature hereby declares that advances in science and technology have led to the development of new devices and techniques for the purpose of eavesdropping upon private communications and that the invasion of privacy resulting from the continual and increasing use of such devices and techniques has created a serious threat to the free exercise of personal liberties and cannot be tolerated in a free and civilized society.

126. California Penal Code Section 638.51(a) proscribes any "person" from "install[ing] or us[ing] a pen register or a trap and trace device without first obtaining a court order."

127. A "pen register" is a "a device or process that records or decodes dialing, routing, addressing, or signaling information transmitted by an instrument or facility from which a wire or electronic communication is transmitted, but not the contents of a communication." Cal. Penal Code § 638.50(b).

128. The Third Parties' cookies and the corresponding software code installed by Defendant on its Websites are each "pen registers" because they are "device[s] or process[es]" that "capture[d]" the "routing, addressing, or signaling information"—including, the IP address and user-agent information—from the electronic communications transmitted by Plaintiff's and the Class's computers or devices. Cal. Penal Code § 638.50(b).

129. At all relevant times, Defendant caused the Third Parties' cookies and the corresponding software code—which are pen registers—to be placed on Plaintiff's and Class

members' browsers and devices, and/or to be used to transmit Plaintiff's and Class members' IP address and user-agent information. *See Greenley v. Kochava*, 2023 WL 4833466, at *15-16 (S.D. Cal. July 27, 2023); *Shah v. Fandom, Inc.*, 2024 U.S. Dist. LEXIS 193032, at *5-11 (N.D. Cal. Oct. 21, 2024).

130. Some of the information collected by the Third Parties' cookies and the corresponding software, including IP addresses and user-agent information, does not constitute the content of Plaintiff's and the Class's electronic communications with the Websites. *In re Zynga Privacy Litig.*, 750 F.3d 1098, 1008 (9th Cir. 2014). ("IP addresses constitute addressing information and do not necessarily reveal any more about the underlying contents of communication...") (cleaned up).

131. Plaintiff and Class members did not provide their prior consent to Defendant's use of third-party cookies and the corresponding software. On the contrary, Plaintiff and the Class members informed Defendant that they did not consent to the Websites' use of third-party cookies by clicking the "Reject All" cookies button in the cookie consent banners.

132. Defendant did not obtain a court order to install or use the third-party cookies and corresponding software to track and collect Plaintiff's and Class member's IP addresses and user-agent information.

133. As a direct and proximate result of Defendant's conduct, Plaintiff and Class members suffered losses and were damaged in an amount to be determined at trial.

134. Pursuant to Penal Code § 637.2(a)(1), Plaintiff and Class members are also entitled to statutory damages of \$5,000 for each of Defendant's violations of § 638.51(a).

Fifth Cause of Action: Common Law Fraud, Deceit and/or Misrepresentation

135. Plaintiff realleges and incorporates by reference all paragraphs alleged herein.

136. Defendant fraudulently and deceptively informed Plaintiff and Class members that he and they could "Reject All" cookies.

137. However, despite Defendant's representations otherwise, Defendant caused third-party cookies and software code to be stored on consumers' devices, and to be transmitted to the

1 Third Parties alongside Private Communications, even after users clicked the “Reject All”
2 cookies button in the Websites’ popup cookie consent banners. These cookies and corresponding
3 software code allowed the Third Parties to access, intercept, read, learn, record, collect, and use
4 Plaintiff’s and Class members’ Private Communications, even when consumers had previously
5 chosen to “Reject All” cookies.

6 138. These misrepresentations and omissions were known exclusively to, and actively
7 concealed by Defendant, not reasonably known to Plaintiff and Class members, and material at
8 the time they were made. Defendant knew, or should have known, how the Websites functioned,
9 including the Third Party’s resources it installed on the Websites and the third-party cookies in
10 use on the Websites, through testing the Websites, evaluating their performance metrics by
11 means of its accounts with the Third Parties, or otherwise, and knew, or should have known, that
12 the Websites’ programming allowed the third-party cookies to be placed on users’—including
13 Plaintiff’s—browsers and devices and/or transmitted to the Third Parties along with users’
14 Private Communications even after users attempted to “Reject All” cookies, which Defendant
15 promised its users they could do. Defendant’s misrepresentations and omissions concerned
16 material facts that were essential to the analysis undertaken by Plaintiff and Class members as
17 to whether to use the Websites. In misleading Plaintiff and Class members and not so informing
18 him and them, Defendant breached its duty to Plaintiff and Class members. Defendant also
19 gained financially from, and as a result of, its breach.

20 139. Plaintiff and Class members relied to their detriment on Defendant’s
21 misrepresentations and fraudulent omissions.

22 140. Plaintiff and Class members have suffered an injury-in-fact, including the loss of
23 money and/or property, as a result of Defendant’s unfair, deceptive, and/or unlawful practices,
24 including the unauthorized interception of his and their Private Communications, including their
25 browsing history, visit history, website interactions, user input data, demographic information,
26 interests and preferences, shopping behaviors, device information, referring URLs, session
27 information, user identifiers, and/or geolocation data, which have value as demonstrated by the
28

1 use and sale of consumers' browsing activity, as alleged above. Plaintiff and Class members
2 have also suffered harm in the form of diminution of the value of his and their private and
3 personally identifiable information and communications.

4 141. Defendant's actions caused damage to and loss of Plaintiff's and Class members'
5 property right to control the dissemination and use of their personal information and
6 communications.

7 142. Defendant's representation that consumers could reject all cookies if they clicked
8 the "Reject All" cookies button was untrue. Again, had Plaintiff and Class members known these
9 facts, they would not have used the Websites. Moreover, Plaintiff and Class members reviewed
10 the Websites' popup cookie consent banners and Defendant's Privacy Notice prior to their
11 interactions with the Websites. Had Defendant disclosed that it caused third-party cookies to be
12 stored on Website visitors' devices that share personal information with third parties, such as
13 performance, targeting, and social media cookies, even after they choose to "Reject All" cookies,
14 Plaintiff and Class members would have noticed it and would not have interacted with the
15 Websites.

16 143. By and through such fraud, deceit, misrepresentations and/or omissions,
17 Defendant intended to induce Plaintiff and Class members to alter their positions to their
18 detriment. Specifically, Defendant fraudulently and deceptively induced Plaintiff and Class
19 members to, without limitation, use the Websites under the mistaken belief that Defendant would
20 not permit third parties to obtain users' Private Communications when consumers chose to reject
21 all cookies. As a result, Plaintiff and the Class provided more personal data than they would have
22 otherwise.

23 144. Plaintiff and Class members justifiably and reasonably relied on Defendant's
24 misrepresentations and omissions, and, accordingly, were damaged by Defendant's conduct.

25 145. As a direct and proximate result of Defendant's misrepresentations and/or
26 omissions, Plaintiff and Class members have suffered damages, as alleged above, and are entitled
27 to just compensation, including monetary damages.
28

1 146. Plaintiff and Class members seek punitive damages because Defendant's
2 actions—which were malicious, oppressive, willful—were calculated to injure Plaintiff and
3 Class members and made in conscious disregard of Plaintiff's and Class members' rights and
4 Plaintiff's and Class members' rejection of the Websites' use of cookies. Punitive damages are
5 warranted to deter Defendant from engaging in future misconduct.

6 **Sixth Cause of Action: Unjust Enrichment**

7 147. Plaintiff realleges and incorporates by reference all paragraphs alleged herein.

8 148. Defendant created and implemented a scheme to increase its own profits through
9 a pervasive pattern of false statements and fraudulent omissions.

10 149. Defendant was unjustly enriched as a result of its wrongful conduct, including
11 through its misrepresentation that users could "Reject All" cookies and by permitting the Third
12 Parties to store and transmit cookies on Plaintiff's and Class members' devices and browsers,
13 which permitted the Third Parties to track and collect users' Private Communications, including
14 their browsing history, visit history, website interactions, user input data, demographic
15 information, interests and preferences, shopping behaviors, device information, referring URLs,
16 session information, user identifiers, and/or geolocation data, even after Class members rejected
17 such cookies.

18 150. Plaintiff and Class members' Private Communications have conferred an
19 economic benefit on Defendant.

20 151. Defendant has been unjustly enriched at the expense of Plaintiff and Class
21 members, and Defendant has unjustly retained the benefits of its unlawful and wrongful conduct.

22 152. Defendant appreciated, recognized, and chose to accept the monetary benefits that
23 Plaintiff and Class members conferred onto Defendant at his and their detriment. These benefits
24 were the expected result of Defendant acting in its pecuniary interest at the expense of Plaintiff
25 and Class members.

26 153. It would be unjust for Defendant to retain the value of Plaintiff's and Class
27 members' property and any profits earned thereon.

1 154. There is no justification for Defendant's enrichment. It would be inequitable,
2 unconscionable, and unjust for Defendant to be permitted to retain these benefits because the
3 benefits were procured as a result of its wrongful conduct.

4 155. Plaintiff and Class members are entitled to restitution of the benefits Defendant
5 unjustly retained and/or any amounts necessary to return Plaintiff and Class members to the
6 position he and they occupied prior to having his and their Private Communications tracked and
7 collected by the Third Parties.

8 156. Plaintiff pleads this claim separately, as well as in the alternative, to his other
9 claims, as without such claims Plaintiff would have no adequate legal remedy.

10 **Seventh Cause of Action: Trespass to Chattels**

11 157. Plaintiff realleges and incorporates by reference all paragraphs alleged herein.

12 158. Defendant, intentionally and without consent or other legal justification, caused
13 cookies to be stored on Plaintiff's and Class members' browsers and devices, which enabled the
14 Third Parties and Defendant to track and collect Plaintiff's and Class members' Private
15 Communications and use the data collected for their own advantage, as described above.

16 159. Defendant was unjustly enriched as a result of its wrongful conduct, including
17 through its misrepresentation that users could reject all cookies and tracking technologies, and
18 through their failure to disclose that Defendant causes third-party cookies to be stored on
19 consumers' devices and browsers, which cause the Third Parties and Defendant to track and
20 collect Plaintiff's and Class members' Private Communications even after consumers chose to
21 reject cookies.

22 160. Defendant intentionally caused third party software code to be stored onto
23 Plaintiff's and Class members' devices, knowing that the code would be executed by those
24 devices. The software code then placed and/or transmitted cookies along with Plaintiff's and
25 Class members' Private Communications to the Third Parties. These intentional acts interfered
26 with Plaintiff's and Class members' use of the following personal property owned, leased, or
27
28

controlled by Plaintiff and other users: (a) his and their computers and other electronic devices; and (b) his and their personally identifiable information.

161. Defendant's trespass of Plaintiff's and other users' computing devices resulted in harm to Plaintiff and other users and caused Plaintiff and other users the following damages:

- a. Nominal damages for trespass;
- b. Reduction of storage, disk space, and performance of Plaintiff's and other users' computing devices; and
- c. Loss of value of Plaintiff's and other users' computing devices.

PRAYER FOR RELIEF

WHEREFORE, reserving all rights, Plaintiff, on behalf of himself and the Class members, respectfully requests judgment against Defendant as follows:

A. Certification of the proposed Class, including appointment of Plaintiff's counsel as class counsel;

B. An award of compensatory damages, including statutory damages where available, to Plaintiff and Class members against Defendant for all damages sustained as a result of Defendant's wrongdoing, including both pre- and post-judgment interest thereon;

C. An award of punitive damages;

D. An award of nominal damages;

E. An order for full restitution;

F. An order requiring Defendant to disgorge revenues and profits wrongfully obtained;

G. An order temporarily and permanently enjoining Defendant from continuing the unlawful, deceptive, fraudulent, and unfair business practices alleged in this Complaint;

H. For reasonable attorneys' fees and the costs of suit incurred; and

I. For such further relief as may be just and proper.

Dated: March 14, 2025

GUTRIDE SAFIER LLP

/s/Seth A. Safier/s/

Seth A. Safier (State Bar No. 197427)

seth@gutridesafier.com

Marie A. McCrary (State Bar No. 262670)

marie@gutridesafier.com

Todd Kennedy (State Bar No. 250267)

todd@gutridesafier.com

Kali R. Backer (State Bar No. 342492)

kali@gutridesafier.com

100 Pine Street, Suite 1250

San Francisco, CA 94111

Telephone: (415) 639-9090

Facsimile: (415) 449-6469

Attorneys for Plaintiff